Yücedağ N, Akkanat-Öztürk EB, 'Data Minimisation and The "Reasonably Be Fulfilled by Alternative Means" Test: A Comparative Study of Turkish And EU Approaches' (2026) 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLT262NYEBAO

EJPLT
ISSN 2704-8012

Data Minimisation and "The Reasonably Be Fulfilled by Alternative Means Test": A Comparative Study of Turkish And EU Approaches

Minimizzazione dei dati e "il test della realizzabilità ragionevole mediante mezzi alternativi": uno studio comparativo degli approcci turchi e dell'UE

NAFIYE YÜCEDAĞ
Assoc. Prof. Dr.
Istanbul University

ELIF BEYZA AKKANAT-ÖZTÜRK
Assoc. Prof. Dr.
Istanbul University

Abstract

This paper analyses data minimisation principle under the GDPR and Türkiye's TDPL. It centers "the reasonably be fulfilled by alternative means test": can a purpose be met with less intrusive processing? Using decisions of the Turkish Data Protection Board, the CJEU, and national authorities, it finds a consistent duty to priorities less intrusive options and clarifies minimizations' interplay with consent. Some bodies demand exploring alternatives; others stress contractual freedom, exposing a tension between autonomy and regulation. The paper argues that even explicit consent cannot displace data minimisation: disproportionate or unnecessary processing remains unlawful. It calls for a nuanced, rights-oriented approach that safeguards dignity and fundamental rights.

© The author(s) 2026, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
L'articolo esamina il principio della minimizzazione dei dati nel GDPR e nella TDPL turca, mettendo al centro "il test della realizzabilità ragionevole con mezzi alternativi": lo scopo può essere raggiunto con trattamenti meno invasivi? Alla luce di decisioni del Garante turco, della Corte di giustizia dell'Unione europea (CGUE) e delle autorità nazionali competenti, emerge un dovere costante di privilegiare opzioni meno intrusive e si chiarisce il rapporto con il consenso. Alcuni organi impongono di esplorare alternative; altri valorizzano la libertà contrattuale, creando tensione tra autonomia e regolazione. Si sostiene che neppure il consenso esplicito elide la minimizzazione dei dati: trattamenti sproporzionati o non necessari restano illeciti. Richiede un approccio sfumato e incentrato sui diritti, che tuteli la dignità e i diritti fondamentali.

Keywords: Data minimisation principle; informational self- determination; fundamental rights protection; human dignity; proportionality

Summary: 1. Introduction. – 2. The Protection of Personal Data: Safeguarding Fundamental Rights and Human Dignity. – 2.1. The Emergence of a Right to Informational Self-Determination. – 2.2. The Data Subject's Ability to Limit Their Own Right. – 3. Data Minimisation: When Adequate? – 3.1. Legal framework. – 3.2. Three Stages of Proportionality Test. – 3.3. Reasonably Be Fulfilled by Alternative Means. – 3.4. Alternatives Tested? – 4. Data Minimisation vs. Consent: Legal Boundaries in Data Protection. – 4.1. The State's Protective Role and Paternalism. – 4.2. Case Examples. – 5. Concluding Remarks.

1. Introduction.

This paper investigates the principle of data minimisation as a safeguard of fundamental rights under both the General Data Protection Regulation (GDPR) and the Turkish Data Protection Law (TDPL). It focuses on the "reasonably be fulfilled by alternative means" test, which serves as the operational filter of necessity within Article 5(1)(c) GDPR and Article 4(2)(ç) TDPL. Controllers must verify whether the intended processing purpose can be achieved by less intrusive alternatives before adopting more invasive measures. Consequently, this mechanism operationalizes proportionality, transforming the abstract principle of data minimization into definitive obligations for data controllers.

The subsequent analysis starts from the premise that Europe and Türkiye's data protection regimes are not built exclusively on freely given nature of consent. They are also structured around non-derogable baseline norms (purpose limitation, fairness, and data minimisation) that continue to apply even when consent has been obtained. This dual structure presents a core challenge: determining how regulators and court should weigh individual autonomy (expressed via consent) against crucial structural protections designed to guard against controller overreach and data subject's potentially harmful choices. To address this question, the paper first situates data minimisation in its broader rights-protective framework, linking it to informational self-determination, autonomy, and dignity. It systematises "the

reasonably be fulfilled by alternative means test" and applies it to practice in Türkiye, and the EU, by referring the decisions of the Turkish Data Protection Authority (TDPA), the CJEU, the Irish Data Protection Commission (DPC) and other national bodies. The comparison reveals both convergence and divergence. The data protection authorities require inquiry into less intrusive alternatives, even testing of it in some instances, indicating that consent does not cure disproportionate processing.

Set against this, certain national courts prioritise freedom of contract and treat consent as determinant factor. The resulting divergence creates the core normative tension in data protection, whether individual autonomy suffices or the law must impose structural limits to secure fundamental rights and human dignity.

2. The Protection of Personal Data: Safeguarding Fundamental Rights and Human Dignity.

The European Union Charter of Fundamental Rights recognizes, in the article 7 and 8 the rights to respect for private and family life and to protection of personal data. Likewise, article 8 the European Convention on Human Rights (ECHR) protects private and family life which covers the processing of personal data. Together, they provide the constitutional framework of European data protection, grounded in autonomy and human dignity.

In the same vein, both the GDPR and the TDPL set out their objectives in Article 1, the GDPR seeks to protect the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data.[1] The TDPL likewise aims to protect fundamental rights and freedoms, with a specific emphasis on privacy in the context of personal data processing.[2]

The protection of personal data is not about safeguarding data as such; it is about protecting the rights and freedoms of the individuals whose data are processed.[3] It is therefore a means to secure fundamental rights, rather than an end.[4] Beyond privacy, data protection contributes to safeguarding personal autonomy, preventing discrimination, ensuring freedom of expression, and ultimately upholding human dignity.[5] In German constitutional doctrine,[6] the

[1] See also GDPR art 1, Recital 1.
[2] See also TDPL art 1.
[3] GG Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014) 130.
[4] See also N Helberger, F Zuiderveen Borgesius and A Reyna, 'The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law' (2017) 54 (5) CML Rev 1427, 1435.
[5] M Oostveen and K Irion, 'The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?' in M Bakhoum and others (eds), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* (Springer 2018) 21.
[6] The German Federal Constitutional Court views personal data protection as a safeguard against human dignity rather than as a means of protecting privacy or property. It emphasises that rights like privacy, data protection, and freedom of expression serve to uphold dignity and are, grounded in data protection principles and self-determination. See A Rouvroy and Y Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the

German Federal Court has highlighted dimensions of the right of personality that include self-determination, self-protection, and self-expression. [7] Accordingly, personal data protection gives effect to the right to informational self-determination.

2.1. The Emergence of a Right to Informational Self-Determination.

The right to informational self-determination was articulated in the German Federal Constitutional Court's 1983 "*Census*" ruling.[8] The Court stressed that processing of personal data must be organised to avoid creating comprehensive personality profiles. In this sense, informational self-determination is a constitutional guarantee of an individual's authority to control the disclosure and use of personal data. Protection is required against unchecked collection, linking and reutilisation of data that would undermine this authority. [9] As the Court emphasised, the right is integral to personal development and to the protection of human dignity.[10]

The right to informational self-determination also encompasses an individuals' control over their personal data. In principle, individuals should have the authority to decide when and to what extent information about their life and relationships is disclosed to the outside world.[11]

In Türkiye, the Constitutions' Preamble identifies the protection of human dignity and personality as a core purpose of constitutional order.[12] Within this framework, Article 20 of Constitution of the Republic of Türkiye expressly guarantees the right to privacy and the protection of personal data. It entitles individuals to be informed about the processing of their data, to access it, and to request its correction or deletion where appropriate. These guarantees are reinforced by the Constitutions' broader protection of human dignity and personality rights, notably in the Preamble and Article 17, which underscore personal autonomy and self-determination as constitutional values.[13]

2.2. The Data Subject's Ability to Limit Their Own Right.

In the German Federal Constitutional Court's census ruling, the disclosure of personal data was treated as an exercise of a fundamental right.[14] Yet the very exercise of that right may endanger its continued existence, for example where disclosure enables extensive profiling or misuse. The states' protective duty is decisive: public authorities must enforce safeguards that preserve the

---

Importance of Privacy for Democracy' in S Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009) 45, 53-54.

[7] U Di Fabio, 'Art 2(1) GG' in R Herzog and others (eds), *Maunz/Dürig: Grundgesetz-Kommentar* (91st edn,
C H Beck 2024) para 166 (beck-online, accessed 22 October 2025).

[8] BVerfG (n 7) 419.

[9] ibid.

[10] ibid.

[11] Rouvroy and Poullet (n 6) 51.

[12] See also The Constitution of the Republic of Türkiye art 17.

[13] See also SK Işık, *Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış* (On İki Levha Yayıncılık 2020) 206 ff.

[14] BVerfG (n 8) 419.

substance of the rights as individuals exercise it.[15] As the German Federal Constitutional Court held in *Lüth* decision,[16] fundamental rights form an objective order of values permeating the entire legal system.[17] Accordingly, they entail positive obligations (*Schutzpflichten*) to organise an effective protective regime.[18] Beyond vertical protection, these duties extend to horizontal relations (*Drittwirkung*)[19] and, in narrowly defined cases, to protecting individuals against self-endangered choices. 20 Thus, although decisional control over personal data rests with the data subject21, dignity-based limits and safeguards may be required where unchecked autonomy would undermine itself or expose others to harm.

3. Data Minimisation: When Adequate?

By restricting the collection and use of personal data to what necessary for a specific purpose, data minimisation principle protects the data subject. In the GDPR and TDPL these principal functions as a "proportionality filter" ensuring that individuals are not exposed to disproportionate risks.

3.1. Legal framework.

Data minimisation is stipulated in Article 5(1)(c) of GDPR: personal data must be "adequate, relevant and limited to what is necessary" based on the purpose for which they are processed. Although the GDPR does not define these terms,

---

[15] F Leinemann, *Personenbezogene Daten als Entgelt? Perspektiven aus Kartellrecht, Verbraucherschutz und Informationsrecht* (Peter Lang 2020) 52.

[16] BVerfG, Urteil vom 15 Januar 1958-1 BvR 400/51 (Lüth) para 20.

[17] BVerfG, Urteil v 1 Dezember 2009 – 1 BvR 2857/07 u a, BVerfGE 125, 39, 78 f; NVwZ 2010, 570, 572. For the view that the concept of positive obligations leads to a narrowing of the scope of rights, see C McKinnon, 'Rights: Their Basis and Limits' in A Mason and R Bellamy (eds), Political Concepts (Manchester University Press 2003) 18–19.

[18] U Di Fabio, *Grundrechtsgeltung in digitalen Systemen: Selbstbestimmung und Wettbewerb im Netz* (CH Beck 2016) 17 ff; HJ Papier, 'Rechtsstaatlichkeit und Grundrechtsschutz in der digitalen Gesellschaft' (2017) NJW 3025, 3030.

[19] Rouvroy and Poullet (n 6) 55; Papier (n 18) 3030; Işık (n 13) 362.For an example of a German Federal Constitutional Court decision addressing the state's obligation to establish a legal framework for protecting fundamental rights and freedoms, see BVerfG, Urteil v 1 Dezember 2009 – 1 BvR 2857/07 u a, NVwZ 2010, 570–580. The Court emphasised that a system protecting fundamental rights exists if:
(1) the state enacts legislation that balances conflicting interests; (2) the legislation is effective and appropriate for safeguarding the relevant rights; and (3) the abstract protection provided by the legislation translates into actual, practical protection. See also BVerfG (n 17) 572.

[20] von Münch introduced the concept of '*Grundrechtsschutz gegen sich selbst*' (protection of fundamental rights against oneself) in response to the question of whether the state (through its legislative, executive, and judicial branches) should protect the holder of a fundamental right against their own will. This concept was developed in the context of debates concerning individual actions affecting their own life or physical integrity. See I von Münch, 'Grundrechtsschutz gegen sich selbst?' in *Festschrift für Hans Peter Ipsen zum siebzigsten Geburtstag* (Mohr Siebeck 1977) 124.

[21] HP Bull, 'Persönlichkeitsschutz im Internet: Reformeifer mit neuen Ansätzen' (2011) NVwZ 257, 258; B Sandfuchs, Privatheit wider Willen? Verhinderung informationeller Preisgabe im Internet nach deutschem und US-amerikanischen Verfassungsrecht (Mohr Siebeck 2015) 128.

they map onto a *proportionality* test. First, personal data must be relevant to the purpose of processing. Second, the data must be necessary to achieve the intended purpose. Unlike the earlier Data Protection Directive 95/46/EC, which only required that data processing not to be "excessive," the GDPR specifies that data processing must be strictly "limited to what is necessary" to achieve the intended purpose. Lastly, the personal data processed must be limited to what is necessary for the purpose.[22]

Despite textual differences, TDPL Article 4(2)(ç) is essentially aligned. Firstly, both provisions require that the processing of personal data must be relevant or connected to its purpose.[23] Secondly, while Article 4(2)(ç) of the TDPL only includes the term "limited," Article 5(1)(c) of the GDPR uses the phrase "limited to what is necessary." However, the absence of the phrase "limited to what is necessary" in Article 4(2)(ç) does not mean that the provision should be interpreted more broadly.[24] In contrast, Article 4(2)(ç) explicitly requires that personal data be processed "proportionately" to the purpose for which they are processed. Ultimately, the proportionality criterion under Article 4(2)(ç) of the TDPL should be understood in a broad sense, encompassing not only adequacy in terms of the processing purpose (a narrower interpretation of proportionality) but also the requirements of being adequate, relevant and limited to what is necessary.[25] Therefore, the concept of proportionality in Article 4(2)(ç) encompasses all three conditions: adequacy, relevance, and limited to what is necessary.

Data minimisation concerns not only the volume of data collected but also the frequency and breadth of use.[26] It further calls for limiting the number of

[22] See also T Frenzel, 'Art 5 DS-GVO' in BP Paal and DA Pauly (eds), *Datenschutz-Grundverordnung (DS- GVO)/Bundesdatenschutzgesetz (BDSG)* (3rd edn, CH Beck 2021) para 34.

[23] Ö Ekmekçi and others, *Kişisel Verilerin Korunması Hukuku* (3rd edn, On İki Levha Yayıncılık 2025) 140.

[24] Ekmekçi and others (n 23) 140.

[25] See also ibid.

[26] In German scholarship, a competing strand reads minimisation as manifesting (but distinct from) general proportionality: even where legitimate aim, adequacy, relevance, necessity and overall proportionality are met, controllers must still reduce data to the greatest extent possible, operating both quantitatively (how much) and qualitatively (which data), across all modalities of processing and, where feasible, via data protection by design (e.g. pseudonymisation/anonymisation). See G Spindler and L Dalby, 'Art 5 DS-GVO-Grundsätze für die Verarbeitung personenbezogener Daten' in G Spindler and F Schuster (eds), *Recht der elektronischen Medien* (4th edn, C H Beck 2019) para 12; H Heberlein, 'Art 5 DSGVO-Grundsätze für die Verarbeitung personenbezogener Daten' in E Ehmann and M Selmayr (eds), *Datenschutz-Grundverordnung* (3rd edn, C H Beck 2024) para 29; S Pötters, 'Art 5 DS-GVO' in P Gola and C Heckmann (eds), *Datenschutz-Grundverordnung–Bundesdatenschutzgesetz* (3rd edn, C H Beck 2022) paras 15, 22–23. The provenance of this reading is traceable to a legislative compromise. The Council resisted a strict minimisation clause, while Parliament's 'alternative-means' refinement channelled proportionality through minimisation. See A Roßnagel, 'Art 5 DS-GVO' in S Hornung and S gen Döhmann (eds), *Datenschutzrecht* (2nd edn, Nomos 2025) paras 116–17. By contrast, this paper treats minimisation as the vehicle through which proportionality is applied to personal-data processing, not a freestanding test. On our reading, however, those very "differences" are nothing more than the components of a structured minimisation assessment. See also European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data protection by design and by default' (ver 2.0, 20 October 2020) paras 48–59 https://edpb.europa.eu/system/files/2021-

affected individuals to the minimum compatible with the purpose, consistent with a data-economy approach.[27]

3.2. Three Stages of Proportionality Test.

The minimisation assessment proceeds in three steps:

(a) relevance, (b) necessity, and (c) adequacy necessity.[28]

(a) Relevance. Personal data must be adequate in relation to the purpose for which they are processed.[29]

(b) Necessity. The data being processed must be relevant to the purpose of the processing.[30]

(c) Adequacy. Personal data can only be deemed appropriate for a purpose if their relevance to the purpose is indisputable.

For instance, when evaluating a job applicant, information about his/her health or political views would generally not be considered adequate or appropriate unless specifically required by the nature of the role.[31] Similarly, requiring employees complete medical files to assess their capacity to work is not considered adequate.[32] Assessing adequacy requires evaluating the degree of interference with fundamental rights and freedoms, including the right to personal data protection. Relevant factors include the nature and sensitivity of the data, the volume collected, whether acquisition was covert, and the technical means employed in processing.[33]

01/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (accessed 17 October 2025).

[27] Pötters (n 26) para 22.

[28] See also P Schantz, 'Art 5 DS-GVO' in HA Wolff, SB and A von Ungern-Sternberg (eds), *BeckOK Datenschutzrecht* (53rd edn, C H Beck 2025) para 24.

[29] The data being processed must be relevant to the purpose of the processing. Relevance is another requirement that serves the principle of data minimisation. It must be present in the data that are appropriate for the purpose. However, even within purpose-appropriate data, there may be irrelevant data that should be excluded from processing. For instance, the (automatic) recording of the receipt of an application to verify compliance with the application deadline may be appropriate for the purpose. However, once the deadline has been met for the application process, recording the receipt of an application is no longer relevant. See also Frenzel (n 23) para 35.

[30] This criterion is engaged where data are already adequate and relevant. For example, is the collection of purpose-appropriate and relevant data in a way that precludes considering all data from the outset. This becomes relevant in cases where limiting the amount of appropriate and relevant data excludes certain references, such as individual prior achievements in an assumed study year abroad for all applicants, for which an overall grade is already provided. See also Frenzel (n 23) para 37.

[31] ibid para 35.

[32] C De Terwangne, 'Art 5' in C Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 317.

[33] F Braun, '§ 47 BDSG' in P Gola and D Heckmann (eds), *Bundesdatenschutzgesetz* (13th edn, C H Beck 2019) para 23.

Finally, although analytically distinct, the three elements often interact in practice.[34] This paper centres on the adequacy criterion[35], understood as requiring that personal data be processed only where the intended purpose cannot reasonably be achieved by other means.[36] Within this structure, the "reasonably be fulfilled by other means" operates inside data minimisation as a primary safeguard[37]: if the aim can be achieved just as effectively through a less intrusive measure, the processing is not adequate for the purpose.[38]

3.3. Reasonably Be Fulfilled by Alternative Means.

On the adequacy account developed above, processing is inadequate where the same aim can reasonably be achieved by a less intrusive route. This section structures "the reasonably be fulfilled by alternative means test", considering the supervisory-authority and judicial decisions. Turkish Data Protection Boards' (TDBP) summary decision, of 20.05.2020 (No 2020/404) applied the data minimization principle to biometric attendance controls, for access and security purposes.[39] Employees were required to provide fingerprints; no explicit consent was obtained, and the privacy notice related to the processing was not presented to the data subject. The controller argued that the data is collected for the purposes of emergency management, physical security, and reporting to authorised bodies. According to the Board less intrusive alternatives (e.g., magnetic cards, RFID tags, SMS-based entry) were available, so collecting biometric fingerprints breached data minimisation.[40] Similarly, the Berlin-Brandenburg Regional Labor Court decided that using biometric data for timekeeping of the employees was not necessary given less intrusive alternatives such as digital cards were available.[41]

---

[34] It has been argued that, despite its brevity, data minimisation merits independent weight; folding materiality and proportionality into purpose limitation finds no support in GDPR Article 5 (1) (b)-(c) or Recital 39. See also Spindler and Dalby (n 27) para 12.

[35] It is stated that GDPR art 5(1)(c) tightens the DPD formula by replacing 'not excessive' with 'limited to what is necessary', and that in practice this constraint is largely absorbed by the adequacy and relevance limbs: Frenzel (n 23) para 37.

[36] See also Frenzel (n 22) para 37.

[37] Spindler and Dalby (n 26) para 12.

[38] See also GDPR arts 5(1)(c) and (e) in conjunction with arts 25(1)–(2), 89(1) (second subpara) and 11(1), which operationalise data minimisation through storage limitation and 'data protection by design and by default', requiring processing and retention only to the extent strictly necessary; Heberlein (n 27) para 31.

[39] Turkish Personal Data Protection Board, 'Summary of the Personal Data Protection Board's Decision dated 01/12/2020 and numbered 2020/915, regarding the biometric data processing for tracking the entry and exit of a municipal employee within the data controller's organisation' https://www.kvkk.gov.tr/Icerik/6872/2020-915 (accessed 22 October 2025).

[40] In a separate case, the Board found that using fingerprint scanners to track municipal employees' entry and exit breached data minimisation. For monitoring working hours, such biometric processing was excessive and unnecessary; less intrusive measures could have achieved the same aim. The ruling reiterates that data collection must remain proportionate and confined to what is necessary for the stated purpose (Turkish Personal Data Protection Board, 'Summary of the Personal Data Protection Board's Decision dated 20/05/2020 and numbered 2020/404, regarding an employer's unlawful processing of an employee's personal data and special categories of personal data without fulfilling the information obligation', https://www.kvkk.gov.tr/Icerik/5496/2019-81-165 (accessed 22 October 2025)).

[41] LAG Berlin-Brandenburg, Urt v 4 Juni 2020-10 Sa 2130/19 paras 76-79.

In another case, the Board reviewed the use of a palm scan system to track the entry and exit of gym members. The TDPB found that the data processing exceeded what was necessary for the processing purpose and that less intrusive alternatives were available.[42] Across these decisions, the common thread is clear: controllers must select means that are adequate to the purpose.

In these cases, the Board did not consider the relevant means to be adequate. Consistently, video surveillance has likewise been addressed in CJEU case law. The data subject filed a lawsuit against the building's co-owner association, requesting a court order for the removal of security cameras. They argued that the video surveillance system infringed upon their right to respect for private life under both EU and national law. In its defence, the controller invoked ongoing vandalism, theft, burglary, noting prior measures had failed. The court applied proportionality to video surveillance: as alternatives (such as intercom and magnetic cards) were attempted but was inadequate and video coverage was confined to only in common areas which reflected the effort to minimize the scope of surveillance. Notably, the Court emphasises the data minimisation principle, which requires the data controller to consider whether the surveillance system could operate only during specific times, such as nighttime or outside working hours. Additionally, the controller must explore the possibility of restricting or obscuring images captured in areas where surveillance is unnecessary.[43] The judgement on video surveillance also underscores case-by-case evaluation.

This decision shows that the existence of reasonable alternatives cannot be assessed in the abstract. Whether a measure is considered intrusive must always be evaluated considering the specific purpose pursued.

The rulings of the Board reflect the CJEU's assessment of proportionality in data processing. the Board, as well as the CJEU emphasized the need to consider less intrusive alternatives to assess the proportionality of the surveillance systems.

---

[42] Turkish Personal Data Protection Board, 'Summary of the Personal Data Protection Board's Decision dated 25/03/2019 and numbered 2019/81 and 31/05/2019 and numbered 2019/165 regarding the processing of biometric data by data controllers providing gym services for the purpose of managing members' entry and exit', https://www.kvkk.gov.tr/Icerik/5496/2019-81-165 (accessed 22 October 2025).

[43] Case C-708/18 *TK v Asociaţia de Proprietari bloc M5A-ScaraA* ECLI:EU:C:2019:1064 (11 December 2019) para 48-51. Similarly, the Lower Saxony Data Protection Authority imposed a fine of €10.4 million on notebooksbilliger.de AG for unlawful video surveillance. For at least two years, the company monitored employees in workplaces, sales areas, and warehouses without a legal basis. Although the company claimed that the cameras were intended to prevent theft and track goods, the authority found the surveillance to be disproportionate: less intrusive measures (such as random bag checks) were not considered, no specific suspicions justified targeted monitoring, the surveillance was neither limited to particular employees nor to a specific time period, and recordings were retained for up to 60 days see Die Landesbeauftragte für den Datenschutz Niedersachsen, 'Videoüberwachung: LfD Niedersachsen verhängt Bußgeld über 10,4 Millionen Euro gegen notebooksbilliger.de' (Press release, 8 January 2021), https://www.lfd.niedersachsen.de/startseite/infothek/presseinformationen/lfd-niedersachsen-verhangt-bussgeld-uber-10-4-millionen-euro-gegen-notebooksbilliger-de-196019.html (accessed 22 October 2025).

In contrast to the Board's approach, the Ankara Regional Court of Appeal[44] decided a case on the merits of freedom of contract. The plaintiff filed a lawsuit against the defendant, argued that the membership agreement had been amended by the introduction of a geometric hand scanning system. The plaintiff sought before the court that the termination of the contract by the defendant was unjustified. According to the plaintiff had not consented to geometric identification method and the contract was terminated unilaterally by the defendant. In its ruling the court decided that the use of the geometric hand scanning system did not constitute an unfair contractual term, and the defendant had the authority to implement security measures under the contract. The court has approached the case from the perspective of the freedom of contract and did not consider the see the clause granted right to amend the contract as an unfair contractual term. Unlike the Board and the CJEU, the court did not engage in a proportionality analysis of the biometric measure or require exploration of less intrusive means. The divergence lies in the starting point: the Board and the CJEU treat proportionality and reasonable alternatives as threshold constraints, whereas the regional court prioritised contractual freedom.

3.4. Alternatives Tested?

A core requirement is to test less intrusive means before resorting to more invasive means. Authorities repeatedly criticise controllers for not invoking less intrusive verification methods before resorting to the more intrusive ones. Controllers must prioritise alternatives and collect only what is "absolutely necessary and proportionate to the aim, consistent with data minimisation principle and limited retention. In line with this, the Irish DCP accepted reliance of article 6(1)(f) GDPR to process photo ID only as a last resort.[45] Airbnb first attempt verification via account data and external data databases: when that failed, it offered verification by a legal name and address addresses; only after that failed too requested a copy of the ID become necessary and was justified.[46]

In another case, the DPC held that Airbnb[47] could not rely on article 6(1)(f) GDPR since no less intrusive verification methods were attempted. Importantly the DPC noted that if those alternatives has been tried and failed, photo ID processing might have been justified. [48] Nonetheless, the DPC found that requesting a complete, unredacted copy of the ID together with a supplemental photograph breached Article 5(1)(c) GDPR, since it exceeded

[44] Ankara Regional Court of Appeal, 3rd Civil Chamber, Case No. 2017/388, Decision No. 2017/401,
Date: April 20, 2017, available at www.lexpera.com (accessed 30 September 2025).
[45] Data Protection Commission, 'Final Decision: Airbnb Ireland UC' (21 June 2023), https://www.dataprotection.ie/sites/default/files/uploads/2023-09/Final%20Decision%20Airbnb%20Ireland%20UC%20-%20June%202023_Redacted%20EN.pdf (accessed 30 September 2025).
[46] DPC (n 45) para 49-50.
[47] DPC (n 45) para 54.
[48] Data Protection Commission, 'Article 60 decision IN-22-9-2' (28 September 2023), https://www.dataprotection.ie/sites/default/files/uploads/2023-11/Art%2060%20decision%20IN-22-9-2%20Redacted.Compressed.pdf (accessed 30 September 2025).

what was necessary for verification and showed no apparent effort to minimise data.[49] As in the related decision, retaining copies of ID documents for the lifetime of the account was deemed unnecessary, lacked adequate justification, and violated the data minimisation principle.[50]

Considered side-by-side, the first DPC decision exemplifies a compliant, gradual application of data minimisation principle, while the second shows that not invoking reasonable alternatives results in breach of the data minimization principle. The rulings required controllers to attempt less intrusive options before requesting to photo ID collection. In short, under article 5(1)(c) GDPR collection must be strictly necessary for stated purpose. This approach is in line with the CJEU's video-surveillance case law. The Court accepted surveillance as proportionate only after measures such as intercoms or magnetic-card entry has proved to be inadequate.[51]

The principal rule is clear: test reasonable less intrusive methods first and limits any processing to what the purpose strictly requires. Failure to comply with the data minimisation principle risks violating data protection rights. Lastly, in this assessment, costs (whether material, financial, temporal, or related to personnel) may be considered. However, they cannot serve as the sole determinant. Yet, the risks associated with personal data processing extend beyond material or economic considerations. The potential harm also involves infringements on fundamental rights and freedoms, such as privacy, autonomy, and human dignity. Accordingly, the evaluation must look beyond cost-efficiency to encompass legal, ethical, and social dimensions.

4. Data Minimisation vs. Consent: Legal Boundaries in Data Protection.

User control is fundamentally anchored in the concept of consent, often serving as a key legal basis for legitimising the processing of personal data. Consent enables the right to self-determination. However, a data protection system based solely on consent cannot fully achieve the purpose of data protection. As *Solove* argued that privacy self-management overemphasizes consent, often overlooking the underlying values of data protection. He argues that, moving forward, the law should abandon this neutrality and establish clear norms with flexible default rules and hard boundaries to address harmful practices.[52]

[49] DPC (n 48) para 68.
[50] DPC (n 48) para 69 ff.
[51] CJEU (n 43) paras 48-51.
[52] DJ Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 Harv L Rev 1880, 1902–03. Nevertheless, despite the recognised role of data protection principles, some authors have argued for minimising or significantly diminishing the role of the data minimisation principle and increasing the accountability and responsibility of data controllers. See FH Cate, P Cullen and V Mayer-Schönberger, Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines (Oxford Internet Institute, December 2013) 11, http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf (accessed 22 October 2025).

4.1. The State's Protective Role and Paternalism.

The state has a duty to protect individuals not only against the actions of others but also, within limits, against the foreseeable consequences of their own choices. The central question is how far the state may constrain individual choices to prevent harm while still respecting voluntary, informed decision-making. Striking the balance means recognising personal autonomy alongside a legitimate public interest in reducing exposure to unnecessary risk. Under the GDPR, user control and data controller responsibility is balanced by providing protections beyond data subject's consent. The balance relies on limits and legitimacy of the restrictions on data subjects' decisions and by the protective state intervention.[53] These restrictions may lead to paternalism which can be defined as the usurpation of one persons' choice of their own good by another person.[54]

While individual control and contractual freedom over data is at the center of data protection law, it does not capture the significance of privacy as a collective good.[55] Privacy extends beyond personal preferences and strategies, encompassing relational and societal dimensions.[56] This necessitates a shift from a purely individualistic perspective to one that recognizes privacy's broader role in safeguarding democratic values and social well-being.[57]

Indeed, focusing only on personal control over data through contractual freedom overlooks privacy's broader impact on society. As some scholars argue an exclusive focus on individual negotiation and autonomy in data privacy fails to account for its broader collective and societal dimensions.[58] As privacy is increasingly seen as a common good or social value,[59] requires recognition of its broader relational and societal aspects beyond the preferences and strategies of individual data subjects and controllers.[60] Data subjects cannot waive the protections provided by key principles such as fairness, purpose limitation, data minimisation, data quality, and data security. These protections are designed to safeguard the rights and freedoms of the data subject, regardless of their consent, reflecting a proactive approach to data protection.[61]

The possibility of risk rests even where consent is given.[62] Data protection law cannot, therefore, be left to individual decision making alone; it must safeguard, fundamental rights and freedoms, at times even against a persons' own decision. As restrictions on individual decision-making aims to protect

[53] C Quelle, 'Not Just User Control in the General Data Protection Regulation' in A Lehmann and others (eds), *Privacy and Identity Management. Facing up to Next Steps* (IFIP AICT 498, 2017) 146.
[54] D Archard, 'Paternalism Defined' (1990) 50(1) Analysis 36, 36 ff.
[55] See Quelle (n 53) 152 ff.
[56] NN Purtova, *Property Rights in Personal Data: A European Perspective* (PhD thesis, Tilburg University 2011) 5.
[57] See also Quelle (n 53) 152 ff.
[58] C Lazaro and D Le Métayer, 'Control over Personal Data: True Remedy or Fairytale?' (2015) 12(1) SCRIPTed 1, 12.
[59] AL Allen, *Unpopular Privacy: What We Must Hide* (Oxford University Press 2011) 13. See Lazaro (n 60) 12.
[60] ibid 12.
[61] Quelle (n 53) 149 ff; Purtova (n 58) 153.
[62] Purtova (n 56) 150.

individuals from the potential consequences of their decisions paternalism becomes more present. This perspective recognizes the inherent vulnerabilities of individuals in the face of powerful data controllers and the need for state intervention to ensure a fair and equitable distribution of power and control over personal data.[63] Data protection is not just about individual rights; rather, it is about fostering a responsible data environment that protects both the individual and society at large.[64]

If the processing is not adequate to the purpose, it can result in unlawful data processing. [65] Even if consent is obtained and meets the legal requirements, the scope of the data processing may still be excessive from an objective perspective. [66] Consent alone does not guarantee lawful data processing if it violates principles like proportionality and purpose limitation.

Contrary to this view the mere existence of a less intrusive method does not automatically render the chosen method unlawful, particularly where explicit consent under Article 9(2)(a) is validly obtained.[67]

In our view, this entirely dismisses a paternalistic approach and implicitly accepts that when consent is present, general principles may not apply. Even when the data subject gives consent based on their free will, there are circumstances where protection is still required. In cases where the data processing is disproportionate, consent alone should not justify this disproportionality.[68] Individuals may require protection even against their own decisions.[69]

This is not paternalistic override of choice, but a structural safeguard against familiar asymmetries and decision frictions in data environments (information overload, default effects, social pressure, bargaining inequality) [70] EU data protection rests on non-derogable baseline norms, most notably purpose limitation and data minimisation principles, that apply even consent is given.[71] Consent may only justify the processing of relevant data, if data minimalization limitations on the scope, frequency, and retention is respected. [72] In short: consent alone does not remedy the disproportionate processing.[73]

---

[63] Quelle (n 53) 153-155.
[64] Purtova (n 56) 207.
[65] See also Frenzel (n 22) para 35; Schantz (n 28) para 26.
[66] ibid para 26.
[67] For a comparable judicial approach in a Member State, see Polish jurisprudence on minimisation, consent and 'reasonable alternatives': Naczelny Sąd Administracyjny (Poland), III OSK 4804/21, https://gdprhub.eu/index.php?title=NSA_-_III_OSK_4804/21 (machine-generated translation) (accessed 23 September 2025).
[68] European Data Protection Board (EDPB), 'Guidelines 05/2020 on consent under Regulation 2016/679' (ver 1.1, 4 May 2020) para 5, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (accessed 16 October 2025).
[69] See also GDPR Recital 43.
[70] See also Roßnagel (n 26) paras 120, 127-128.
[71] For discussion of dignity as a constraint and the State's role in limiting alienation of personal data see also O Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015) 244 ff.
[72] EDPB (n 68) para 5; See also Roßnagel (n 26) paras 127-128.
[73] See also Roßnagel (n 26) para 127.

4.2. Case Examples.

In a decision, the Board[74] clarified that that even if the members provide explicit consent, the processing of biometric data for accessing a gym does not align with the principle of data minimisation. TDPB found that conducting fingerprint/palm print scanning for security purposes when entering a gym constitutes an excessive intervention in the individual's right to the protection of their personal data since a less intrusive method could be chosen for security at the gym entrance. Even if the data subject's consent is obtained and is freely given, the processing will still be considered contrary to general principles if the processed data exceeds what is necessary for the purpose.

In this case, the bank required customers setting up a digital password via their Turkish ID card to provide consent for the processing of facial data. If consent was withheld, the service could not proceed in that channel, though the same service was still accessible through other routes, namely branch banking and telephone banking. The Board found that these alternative channels is sufficient to consider the service is conditioned on biometric consent. Since the communication of these alternatives to customers was not clear, the Board only advised the bank to improve transparency and user guidance.[75] Although the decision does not make an explicit reference to the data minimization principle, it was implied that the bank has respected this principle. At that case data minimization principle was not breached since biometric verification was linked to a legitimate aim namely safeguarding the security of financial data and banks are obliged employ at least two independent identity verification mechanisms in electronic banking one of which can be biometric verification.

These cases exemplify the critical challenge of balancing individual autonomy, consent, and data protection principles.

The contrast with the gym case is instructive. In both cases consent was obtained yet the legality of processing was questioned based on the data minimization principle. The first case shows that explicit consent does not justify disproportionate data processing. even with consent of the data subject. The use of biometric data was found not to justify ensuring physical security of a gym and verify customers' identities.

In contrast, the bank case justifies the interference based on the objective of safeguarding financial data security, particularly given the availability of alternative verification methods. Since this case concerns a regulated sector, it is likely that the measures taken for data security in the banking industry were also considered. The level of interference and its proportionality should be assessed by considering factors such as the nature and volume of the data

[74] Turkish Personal Data Protection Board, 'Summary of the Board's Decision dated 27 February 2020 and numbered 2020/167, regarding a data controller providing gym services who processes biometric data to monitor the entry and exit of its members', https://www.kvkk.gov.tr/Icerik/6738/2020-167 (accessed 23 September 2025).

[75] Turkish Personal Data Protection Board, 'Summary of the Personal Data Protection Board's Decision dated 3 August 2023 and numbered 2023/1310, regarding the processing of personal data using facial data while setting a digital password in a bank's mobile application', https://www.kvkk.gov.tr/Icerik/7775/2023-1310 (accessed 23 September 2025).

processed, whether the data was obtained covertly, and the technical methods used in processing.

5. Concluding Remarks.

EU data protection law is not built solely on consent but on non-derogable baseline norms that continue to apply even when consent exists. Among these, purpose limitation and data minimisation are most central. Consent may authorise a purpose and permit the processing of relevant data, yet minimisation still requires that the scope, frequency, and retention of data remain limited to what is genuinely necessary for that purpose. The approach therefore combines two elements: individual control through consent and structural constraints through mandatory principles. This dual structure prevents data protection from collapsing into a purely voluntarist model, which would leave persons to bear risks they cannot realistically evaluate or mitigate. At the same time, it avoids turning the law into a paternalistic restriction of autonomy, as the individual still plays a role in authorising the purposes for which data may be processed.

Within this framework, the "reasonably be fulfilled by alternative means test" is satisfied if (i) the purpose is defined clearly and legitimate, (ii) the method chosen is proportionate to that purpose, and (iii) reasonable less intrusive alternatives are available or demonstrably failed. The assessment of reasonable less intrusive alternatives involves the cost and practical feasibility of the means, as well as the broader impact of the processing through that means on the fundamental rights and freedoms of data subjects. While assessing the impact of the means on the fundamental rights and freedoms of data subjects the nature of the data, the volume of the date, whether the collection occurs in clandestine way, and the technical means employed in the processing can be considered. Data minimization under Article 5(1)(c) GDPR is thus not measured by cost-efficiency alone, but also on the impact of the processing through the means used for processing on the fundamental rights and freedoms of data subjects.

Moreover, the balance lies in ensuring that individual choice remains central but is not left unprotected. Consent may open the door to processing, but it is data minimisation that sets the boundaries and keeps processing within lawful and fair limits. This layered approach captures the essence of European data protection: a system that respects autonomy, secures fundamental rights, and addresses the power asymmetries of the digital environment.